Příloha č. 1 – požadavky na monitorovací systém

(níže uvedeným požadavkům odpovídá např. software firmy EKRAN EKS-TSA Jump Box6 Server Agent)

I. Obecné požadavky

- Dodávka a nasazení systému pro kompletní dohled nad veškerými externími přístupy do IT infrastruktury zadavatele.
- Implementace řešení do IT prostředí kupujícího - virtualizované prostředí VMware ESXi, verze 6.5.0 build 13932383 případně vyšší, včetně následné podpory celého řešení.
- Monitorování všech přístupů realizovaných přes jeden virtualizovaný terminálový server.
- Kontrola správné konfigurace virtualizovaného Terminal serveru a jeho případné nastavení.
- Řešení musí umožnit nahrávání všech (i souběžně probíhajících) vzdálených připojení včetně záznamu textu pro rychlejší orientaci v nahrávkách.
- Nahrávky budou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou následně dlouhodobě uchovávány.
- Řešení, pokud není schopné pracovat s DB Oracle, musí umožnit uložení záznamů do své interní DB, případně do jiné DB bez dalších nákladů pro zadavatele.
- Systém bude zajišťovat nahrávání uživatelských relací – snímáním obrazovky a volitelně logování uživatelského vstupu (tzv. key logging).
- Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu bude nahrávána a bude jednoznačně přiřazena konkrétní osobě.
- Technická podpora/maintenance dodaného řešení na 1 rok s možností prodloužení.
- Dodané řešení nesmí být řešeno formou pronájmu, po skončení technické podpory musí být dále schopno pracovat.

II. Technické požadavky

- Software umožňující auditování, monitoring a nahrávání uživatelských relací:
  - Auditování, monitoring a nahrávání aktivit administrátorů na serverech při vzdáleném i lokálním přihlášení.
  - Auditování, monitoring a nahrávání aktivit externích uživatelů vykonávající vzdálenou správu v LAN Zadavatele, Monitorování a nahrávání uživatelských relací v rámci běžných platforem: Unix / Linux / Windows / Citrix.
- Každá z nahraných uživatelských relací je indexována pomocí textových metadat (názvy oken, textové řetězce, názvy stisknutých tlačítek, …), tak aby bylo zřejmé, k jakým aktivitám během relace došlo, aniž by bylo nutné shlédnout nahranou videosekvenci. V metadatech je možné fulltextově vyhledávat.
- Schopnost zpětně přehrávat uživatelské relace ve formě videosekvence.
- Schopnost exportu nahraných uživatelských relací (včetně snímků obrazovek a metadat) pro tvorbu dokumentace nebo prokazování incidentů.
- Autentizace přístupu ke všem komponentám je řízena adresářem LDAP (eDirectory), nebo ActiveDirectory.

- Aplikace musí umožnit správu rolí (auditor, správce, apod.).
- Uživatelé mohou být nástrojem při navázání relace upozorněni na skutečnost, že jejich aktivita je nahrávána.
- V rámci nahrávky mohou být zaznamenávány uživatelské vstupy (tzv. key logging).
- Možnost sekundární formy autentizace pro jednoznačnou identifikaci administrátora v případě využití sdílených administrátorských uživatel.
- Integrovaný alerting na základě definovaného nestandardního chování uživatelů (identifikace netypické/nestandardní aktivity uživatele, například spuštění editoru registrů).